Testimony before the Intelligence, Information Sharing and Terrorist Risk Assessment Subcommittee of the House Committee on Homeland Security

13 September, 2006

Maureen Baginski, Director, Intelligence Sector, BearingPoint, Incorporated

Chairman Simmons, Ms. Lofgren and Subcommittee members, it is my pleasure to appear before you today to discuss the vital issue of information sharing and enabling technology. I served in the United States Intelligence Community for a total of 27 years, most recently as Director of Signals Intelligence at the National Security Agency and Executive Assistant Director for Intelligence at the FBI. In those positions I both used and managed the delivery of many information technology systems--some of them successful and some of them not. My purpose today is to share with the Subcommittee lessons learned from those experiences that may be of use to the Department of Homeland Security as it moves ahead with the development and deployment of vital information sharing systems. Those lessons learned have been considerably enriched by my tenure at BearingPoint, where I have been exposed to the power of the commercial sector's approach to similar challenges.

Information is a tool that each of us uses every day to inform decision making. Our decision making domains are often very different, and we tailor available information to our specific roles and responsibilities at any given point in time. The quality of our decisions is dependent on the quality of information available to us. We do not necessarily need more information; we need the right information for our decision domain. This is the core challenge facing all information sharing systems today. Among the painful lessons learned in recent years is that information does not come marked "terrorism information", "war fighting information", "policy information", "criminal information", or "natural disaster information". The threats facing our nation today are global in nature and no single source of information or single organization can defend against these threats alone. It will take all of us working as a network to defend against these global threats and the goal of information sharing programs is to create that network.

For the producers of information—particularly those in the Intelligence Community--, the new threat environment requires that they judge their performance not on information output, but on the outcomes their information enables for the nation. First and foremost that means that information stewards—whether they are at the federal, state, local or tribal level-- must invest considerable time and effort in understanding the domains of those who must act on their information. Then they must provide information to those users in the form that is of most utility to them.

At the risk of gross oversimplification, intelligence is vital information about phenomena that would do our nation harm. The value of intelligence is judged by the user of that intelligence and not by its producer. Intelligence protects our nation in three ways: by the information it provides, by providing it a way that safeguards the rights of all U.S. citizens, and by spending taxpayer money responsibly. These are shared imperatives and each must be fulfilled. In today's world of global threats, the user base of intelligence has been greatly expanded, extending now from the President, to the soldier, to the patrolman and beyond. For example, a detailed, scientific paper about RICIN written at the classified level may be of enormous value to our scientific and health communities. For our patrolmen, the most valuable information in that report may be the unclassified photograph of the castor bean plant that could be used at "roll call" to inform the officers to be on the alert for it in the course of normal duties, i.e. in their unique decision domain. With timely, actionable information tailored to the operating environment of individual users we are more likely to be successful in getting inside and ahead of the adversaries' decision making cycle and prevent the harm they would do.

The creation of an information sharing environment with the characteristics described above is a complex undertaking and has many inextricably linked components related to people, processes, organization and technology. Information systems rarely "fail" because of technology. Information sharing systems are essentially "dumb"; they do only what business processes and business rules tell them to do. They are more likely to fail because:

1) their purpose is unclear
2) they fail to involve all stakeholders, particularly the user community
3) the changes in organizational culture that they require have not been communicated or prepared for effectively
4) the business processes that they are to enable have not been defined.
5) they lack sponsorship at all levels of leadership
6) weak program management

Below are examples of successes and failure in each of the dimensions listed above.

Clear Purpose

The need for a clear understanding of the purpose of an information sharing system is critical to its success. Often this purpose is sketched out at a high level using a Concept of Operations or Conops. The Department of Justice took the Conops approach to information sharing and began in 2003 to develop within DOJ (with DHS and state, local and tribal law enforcement participation) the Law Enforcement Information Sharing Plan, or LEISP. The guiding principle of LEISP was that there would be a "one DOJ" information sharing platform for DOJ partners in law enforcement. The Conops process was not without considerable pain and difficulty, and completion took well over a year,

largely because of very understandable concerns about the how information would be used, and what might be fairly characterized as “turf issues”. In addition, In information the CONOPs’ completion was delayed by concerns that it lacked sufficient detail to be implemented. The effort was very ably led by DOJ CIO Vance Hitch and had the personal sponsorship of Deputy Attorney General James Comey.

Just as the Conops effort appeared to be foundering, Deputy Attorney General Comey made an important decision. Essentially he decided that the details desired by those working on the Conops could be developed more quickly if the concepts were tested in a real world environment. In partnership with then Secretary of the Navy Gordon Englund, DAG Comey ordered all DOJ elements to make specific information available to a functioning information sharing system in Seattle called LINX. LINX unified federal and state and local law enforcement information in a single system to improve information sharing. DAG Comey personally sponsored the project, set deadlines, and made hard decisions in the face of some resistance and legitimate concerns about the resource demands of the program. In the end, deadlines were met and DOJ was able to implement the LEISP concepts, now called “one DOJ” in a real world system. This is an excellent example of both strong leadership and the utility of testing concepts in small pilot offerings to inform further development of information sharing processes.

Involve All Stakeholders

In 27 years of Federal service, the best example I have seen of the power of involvement of all stakeholders in an information sharing has been in the Law Enforcement Community.

The FBI’s Criminal Justice Information Services (CJIS) Division serves as the focal point and central repository for criminal justice information services within the FBI and is responsible for day-to-day management of the following programs administered by the FBI for the benefit of local, state, tribal, federal, and foreign criminal justice agencies:

Integrated Automated Fingerprint Identification System (IAFIS)
The National Crime Information Center (NCIC)
Unified Crime Reporting Program
National Instant Criminal Background Check System (NICS)
Law Enforcement National Data Exchange (N-DEx)
Law Enforcement on Line (LEO)

CJIS administers these systems through an Advisory Process that has existed since the inception of these systems in 1969. The philosophy underlying the advisory process is one of shared management; that is the FBI along with local and state data providers and system users share responsibility for the operation and management of all systems administered by the FBI for the benefit of the criminal justice community. The CJIS Advisory Process consists of two components: the Working Groups and the Advisory Policy Board (APB). The CJIS Working Groups review operational, policy, and technical issues related to CJIS programs and policies and make recommendations to the APB or to

one of its subcommittees. All fifty states, as well as U.S. territories and the Royal Canadian Mounted Police are organized into five working groups. The APB is responsible for reviewing appropriate policy, technical, and operational issues related to CJIS programs and for making appropriate recommendations to the Director of the FBI.

Law Enforcement On-line (LEO) is a system developed under this process. LEO is very much like HSIN and provides a secure information sharing capability based on communities of interest. In the early stages, LEO was not universally well received by the user community. First, it was not considered user friendly, particularly in its password regimen. Second, the information on LEO was not of sufficient value to the law enforcement community to make the pain of the password regimen worth the effort. Through the APB, CJIS worked to modify the password regimen and ensure that information placed on LEO was of more value to the user community. These improvements made LEO of more utility and usage increased. The process of improving and refining LEO continues today through the APB process.

Although this process has not been without points of pain, it has engendered both trust and mission success. The CJIS process has created a shared governance model in which all users agree on the elements of information to be shared, understand that the "price of admission" to system access is to flag and tag that information such that it is available to all, and defines sanctions for misuse of information that is shared. This is a powerful model that could be leveraged or emulated in DHS's continued work on HSIN and related systems.

Change Management

Information sharing on the scale required by the new global threat environment is new for the vast majority of participants. Change of this magnitude must be managed every bit as carefully as the technology implementation itself. For many the change will be threatening or not understood. Success hinges on communication, training and clarity of vision.

Virtual Case File (VCF) may seem like an unlikely choice as an example of good changes management process, but it is instructive. As the Subcommittee is aware, Director Mueller's transformation of the FBI from a law enforcement only to a law enforcement and intelligence entity has two core pillars: intelligence and information technology. Recognizing the magnitude of the change required in FBI operations, in 2003 Director Mueller required that all senior managers in the FBI attend a week-long course at North Western's Kellogg School of Management, entitled "Navigating Strategic Change". In those sessions managers received presentations on both VCF and Intelligence, and discussed the imperatives for each. In addition, managers worked through a series of case studies designed to provide them with the tools to manage the cultural change that both VCF and the new intelligence mission would entail. Managers

then returned to their operational duty stations with the mandate to "cascade" the change throughout all levels of their organization.

This well-planned and executed component of the change management process, however, was not sufficient to make VCF a success.

Define Business Processes

According to the FBI's own analysis, one of the major contributing factors to the failure of VCF was the lack of well-defined and agreed upon business processes to drive and define the requirements for the system. As the Subcommittee is aware, VCF was the third component of the FBI's Trilogy Program—a program designed to deliver the core functionality for an FBI information technology enterprise. Phases I and II of that program (the backbone and computer hardware) were delivered on time and within budget. Phase III, VCF, was an FBI enterprise-wide case management system. That system was not a success and following an extensive independent review, was terminated. The independent review cited two primary reasons for the termination recommendation:

1) it appears that either the FBI was unable to clearly communicate requirements so that they were completely understood by the Contractor, and/or
2) that the Contractor deviated from those requirements without exercising change management and ensuring customer buy-in along the way.

The Trilogy Program illustrates clearly the criticality of business process definition in the delivery of information sharing systems. The information backbone and hardware could be delivered without critical business process definition and were delivered successfully. VCF was a collection of software applications that required a clear set of business rules to which system developers could map data. In the absence of agreed upon enterprise-wide business processes, those business rules could not be developed. The FBI learned a hard lesson from this experience and has launched an enterprise-wide business process definition initiative to drive the development of the Sentinel system. The success of that program will depend largely on the success of that process.

Leadership Sponsorship

Leadership sponsorship and commitment is the key to the success of any initiative, but may be even more critical for information sharing initiatives that challenge existing views about data ownership. There are many examples of strong senior leadership and its positive effect on information sharing capabilities, such as the DOJ LEISP pilot cited above led by DAG Comey. Another example is the Intelligence Community's intranet, called INTELINK. INTELINK was designed to create an intelligence product sharing capability across the IC and was personally championed by then D/DCI Admiral William Studeman in the early 1990's. At the time there was not only considerable resistance to

the concept, but real obstacles to implementation in then extant IC information sharing policies. D/DCI Studeman carefully steered the initiative through the policy issues, made hard decisions, and mandated the implementation across the Intelligence Community. Today the majority of IC members cannot remember a time when there was not an INTELINK, but its implementation took time, patience, and most of all strong leadership support.

Strong Program Management

The FBI considers that lack of strong program management practices to be a root cause of the VCF failure and cites weaknesses in acquisition management and requirement/change management as particularly critical. At the highest level the FBI cites shortcomings in three areas:

1. The quality and ability of people to motivate and manage multi-disciplined teams of diverse specialties
2. The lack of effective program management processes and methodology
3. The lack of sufficient technology to forecast and measure risk, to manage and monitor earned value, and to perform to requirements.

Given these concerns, the FBI has focused corrective action plans and initiated a number of programs to guard against a recurrence of these problems. In acquisition management, the FBI has restructured and modernized the acquisition management process, including career development for contracting officers. Most importantly, the FBI has learned the definition of requirements in acquisition documents is paramount and has invested experience personnel in managing requirements definition. Simply stating needs and detecting what is deemed a responsive offering does not guarantee mutual understanding between the Government and the Contractor. The FBI is committed to taking whatever amount of time it takes to come to a meeting of the mind on requirements, and only then to establish contractual agreements, penalties, and awards.

For requirements management, the FBI has learned that program management is a professional discipline requiring specialized talents and training in which it must invest. Clear requirements definition and the inevitability of changes in those requirements must be understood and managed effectively. Integral to that process is a comprehensive Change Management Plan, according to which requirements changes are introduced, evaluated for impacts to schedule and budget, and agreed upon. In addition, the new program management process includes the creation of a risk management matrix that identifies each risk and the projected and actual cost of risk mitigation.

A Way Ahead

Information sharing/access is a challenge faced by virtually every organization in the world. For that reason, many commercial technology organizations like BearingPoint are

devoting considerable effort to developing solutions for the challenges inherent in information sharing systems. One promising solution centers on the development of a series of "maturity models" that both assess the ability of organizations and communities to implement complex information sharing programs, and provide specific criteria for moving from the lowest to the highest maturity level. Because the successful implementation of information sharing systems depends on people, processes, organizations and technology, the maturity models measure readiness in all of those dimensions.

The "maturity model" approach is outlined below:

Enterprise Maturity Model

Organizational Maturity-The degree of maturity related to leadership, strategic direction, human capital management, and communication and collaboration
Business Process Maturity-The degree of maturity of business process management and automation
Information Maturity-The degree of maturity of data and information quality and availability
Application Maturity-The degree of maturity of applications supporting the business processes
Technology Maturity-The degree of available shared services and components use
Security Integration-The degree of security pervasiveness
Provider Maturity-The degree of ownership of information technology resources

Information Sharing Maturity Model

Policy/Strategy Maturity- The degree to which information sharing policy, strategy and metrics has been defined and are understood across all participating organizations

People/Organization Maturity-The degree to which leadership, strategic direction, human change management, communication, and training are being effectively implemented across all participating organizations
Process Maturity-The degree to which information sharing processes are defined and implemented in a consistent fashion across all participating organizations
Governance Maturity- The degree to which governance processes are in place for coordinating and controlling information sharing activities across all participating organizations
Architecture Maturity- The degree to which standards, best practices, guidelines, reference architectures, etc have been defined ad agreed upon so as to provide guidance to the participation organizations so that they can efficiently and effectively implement the information sharing initiatives
Technology Maturity- The degree to which the participating organizations have the information services, technical infrastructure, and security in place to efficiently and effectively support the information sharing initiatives

The above maturity models must be supported by performance measures.

Information Sharing Metrics Library and Process Library

Outcome Metrics-Measures the extent to which information sharing initiatives improve mission/government/department/agency outcomes

User Metrics-measures the extent to which users are provided with or have access to the information they need to get their job done effectively

Process Metrics-measures the extent to which information sharing initiatives improve key information sharing processes (many of these processes take weeks today because they are done manually—these metrics will measure the effectiveness of automating the processes across multiple agencies)
Information Metrics-measures the extent to which information is accessible, visible, understandable, and trustworthy

Finally, it is important to note that in the development of information sharing systems, where you are is very much where you sit. Now, sitting on the outside, it is easy to articulate issues and offer solutions. I have also been on the inside and have lived with the unforgiving operational tempo that often confounds the best intentions to remain focused on these core issues. Success will require a partnership of all parties and all branches of government to provide critical oversight, resources and time necessary to implement these critical systems. This hearing is a measure of your commitment to that partnership. Thank you for allowing me to participate.